



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/816,080      | 03/26/2001  | A-jung Kim           | 030681-291          | 7143             |

21839 7590 07/14/2004

BURNS DOANE SWECKER & MATHIS L L P  
POST OFFICE BOX 1404  
ALEXANDRIA, VA 22313-1404

|          |
|----------|
| EXAMINER |
|----------|

DADA, BEEMNET W

|          |              |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2135

DATE MAILED: 07/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/816,080

Applicant(s)

KIM, A-JUNG

Examiner

Beemnet W Dada

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 26 March 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-6 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-6 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>9</u> . | 6) <input type="checkbox"/> Other: _____  |

### DETAILED ACTION

1. Claims 1-6 have been examined.

#### ***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lo et al. (hereinafter referred to as Lo) (US Patent No. 5,732,139) in view of Mazourenko et al. (hereinafter referred to as Mazourenko) (US Patent No. 6,272,224 B1).

4. As per claim 1, Lo teaches a key agreement method for secure communication in a multiple access system, the key agreement method comprising the steps of:

a first user (Alice) encoding a signal from a source by a bit sequence and transmitting the signal [column 8, lines 11-17, lines 64-67 and column 5, lines 36-39];

a second user (Bob) who is a legitimate counterpart of the first user decoding the transmitted signal and measuring the decoded signal [column 8, lines 18-21, lines 64-67 and column 5, lines 40-44];

the second user adopting only bits having the measured value beyond the threshold value which is predetermined [column 6, lines 17-31 and column 8, lines 55-60]; and

the first and second users taking the adopted bits as a key string, and discarding the remaining bits [column 8, lines 62-67 and column 6, lines 32-37].

Furthermore, Lo teaches the method further comprising the second user informing the first user the basis for his measurements but not the measurement results, the first user tells the second user whether he has performed the correct measurement and the first and second user using the data where the first user has measured correctly as a key string [column 8, lines 24-35 and column 5, lines 45-55]. Lo does not explicitly teach the second user informing the first user that the bits adopted are the n-th bits in the transmitted bit sequence, not telling the values of the bits and adopting the bits as a key string. However, Mazourenko teaches a method of key distribution wherein a second user informing a first user that the bits adopted are the n-th bits in the transmitted bit sequence, not telling the values of the bits (i.e., informing when a photon is detected not revealing the phase used) and adopting the bits as a key string [column 4, lines 37-41 and column 8, lines 54-67]. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a key distribution method wherein a second user informs a first user that the bits adopted are the n-th bits in the transmitted bit sequence, not telling the values of the bits (i.e., informing when a photon is detected not revealing the phase used) and adopting the bits as a key string as per teachings of Mazourenko and implement it into the key distribution method taught by Lo, because the modification further secures the method from eavesdropping on key agreements between a sender and a receiver by not revealing values of phase used.

5. As per claim 2, the combination of Lo and Mazourenko teaches the method as applied to claim 1 above. Furthermore, Lo teaches the method further comprising the steps of:

selecting a subset of bits from the key string shared by the first and second users and checking errors [column 8, lines 46-48];

if the error rate obtained is below a tolerable level, considering the transmission safe, accepting the key string and obtaining a refined key string with amplification such as error correction process [column 8, lines 46-63]; and

discarding the key adopted in the step if the error rate obtained in exceeds the tolerable level, returning to the first step and performing through until getting the key string which satisfies the condition [column 8, lines 46-65].

6. As per claim 3, the combination of Lo and Mazourenko teaches the method as applied to claim 1 above. Furthermore, Lo teaches the method wherein the signal transmitted is susceptible to noise [column 2, lines 54-57].

7. As per claim 4, the combination of Lo and Mazourenko teaches the method as applied above. Furthermore, Mazourenko teaches the method wherein the second user uses a receiver affected by mutual modulated noise by another transmitter [column 10, lines 15-25, and column 5, lines 27-39].

8. As per claims 5 and 6, the combination of Lo and Mazourenko teaches the method as applied above. Furthermore, Lo teaches the method wherein threshold value is determined by the second user considering at least a transmission rate, transmission error rate and a degree of security [column 6, lines 17-20].

**Conclusion**

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO form 892.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (703) 305-8895. The examiner can normally be reached on Monday - Friday (8:30 am - 6:00 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

July 9, 2004

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2103